Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application. Claim 15 is presented on page 6 in unmarked form for Examiner's convenience.

Listing of Claims:

Claims 1-14 (Canceled)

15. (currently amended) An encryption circuit for simultaneously processing various encryption algorithms, the encryption circuit adapted to be coupled to a host computer system, the encryption circuit comprising:

an input/output module coupled to the host computer system ~~via~~ through a dedicated bus,

the input/output module handling data exchanges between the host system and the encryption circuit ~~via the input/output module and the dedicated bus and~~,

the input/output module comprising a microcontroller and a microcontroller control memory, the microcontroller control memory providing storage for program control of the microcontroller;

an encryption module ~~coupled to the input/output module,~~

~~said encryption module controlling~~ performing data encryption and decryption operations, as well as storage of all sensitive information of the encryption circuit; and

isolation means ~~operatively~~ comprising a dual port memory connected between the input/output module and the encryption module, the isolation means ~~configured to make~~ ensuring that the sensitive information stored in the encryption module is inaccessible to the host computer system,

~~and for ensuring the operations performed by the input/output module and encryption module can be carried out in parallel~~

the dual port memory enabling parallelism between 1) the data exchanges performed by the input/output module and 2) the data encryption and decryption operations performed by the encryption module.

Claims 16-19 (Canceled)

20. (currently amended) An encryption circuit as set forth in claim [17] 15, wherein the encryption module comprises:

a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms, and being coupled to the first bus of the dual port memory;

a second encryption sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled to the first bus of the dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory; and

a CMOS memory, coupled with the dual-port memory via the first bus of the dual-port memory, the CMOS memory containing the encryption keys accessible during execution of encryption algorithms by the first and second encryption sub-modules and the CMOS memory connected to be reset upon detection of an alarm condition protecting the encryption keys from unauthorized access and use.

21. (currently amended) An encryption circuit according to claim [18] 20, wherein the first encryption sub-module comprises an encryption component coupled to the dual-port memory via the first bus of the memory, the encryption component comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and the second encryption sub-module comprises at least two encryption processors, respectively dedicated to the processing of asymmetric encryption algorithms, the encryption processors being coupled to ~~the~~ the first bus of the dual-port memory via the internal second bus of the second sub-module and a bus isolator that isolates the second bus from the first bus of the dual-port memory.

22. (Previously Presented) An encryption circuit according to claim 21, wherein the encryption processors of the encryption module are of the CIP configuration.

23. (Previously Presented) An encryption circuit according to claim 21, wherein one of the two encryption processors is of the CIP type, and in that the other of the two encryption processors is of the ACE configuration.

24. (Previously Presented) An encryption circuit according to claim 21, wherein one of the two encryption processors is of the ACE configuration comprising a field programmable gate array (FPGA).

25. (Previously Presented) An encryption circuit according to claim 24, wherein the encryption component is of the SCE configuration.

26. (Previously Presented) An encryption circuit according to claim 25, wherein the encryption component comprises a field programmable array (FPGA).

27. (Previously Presented) An encryption circuit according to claim 26, wherein the second encryption sub-module comprises a flash memory PROM and an SRAM memory coupled to the second internal bus of the sub-module.

28. (Previously Presented) An encryption circuit according to claim 21, further comprising a CMOS memory containing security keys and security mechanisms that trigger a reset mechanism of the CMOS memory in case of an alarm protecting the encryption keys from unauthorized access and use.

29. (Previously Presented) An encryption circuit according to claim 15, wherein the microcontroller comprises:

an input/output processor and a PCI interface integrating DMA channels responsible for executing the data transfers between the host computer system and the circuit; and the memory comprises a flash memory containing the code of the input/output processor and a static random access memory that receives a copy of the contents of the flash memory upon startup of the input/output processor.

30. (Previously Presented) An encryption circuit according to claim 15, comprising a serial link connected to input basic keys through a secure path independent of the dedicated PCI bus, said link controlled by the encryption module.

31. (Previously Presented) An encryption circuit according to claim 30, wherein the serial link (SL) allows downloading of proprietary algorithms into the first encryption sub-module.

32. (Original) An encryption circuit as set forth in claim 15, further including a card supporting the circuit.

33. (Original) An encryption circuit as set forth in claim 18, further including a card supporting the circuit.

34. (Original) An encryption circuit as set forth in claim 21, further including a card supporting the circuit.

35. (New) An encryption circuit for simultaneously processing various encryption algorithms, the encryption circuit adapted to be coupled to a host computer system, the encryption circuit comprising:

an input/output module coupled to the host computer system through a dedicated bus which provides direct access by the encryption circuit to the host system,

the input/output module handling data exchanges between the host system bus and the encryption circuit;

the input/output module comprising a microcontroller and a microcontroller control memory, the microcontroller control memory providing storage for program control of the microcontroller;

an encryption module performing data encryption and decryption operations, as well as storage of all sensitive information of the encryption circuit, the encryption module comprising:

a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms;

a second encryption sub-module, dedicated to the processing of asymmetric encryption algorithms; and

a CMOS memory containing the encryption keys accessible during execution of encryption algorithms by the first and second encryption sub-modules and the CMOS memory connected to be reset upon detection of an alarm condition protecting the encryption keys from unauthorized access and use; and

isolation means comprising a dual port memory connected between the input/output module and the encryption module, the dual port memory being coupled to a first bus which couples to the first encryption sub-module, said second encryption sub-module and a second bus which couples to the input/output module, the isolation means ensuring that the sensitive information stored in the encryption module is inaccessible to the host computer system and is protected from unauthorized access and use, and

the dual port memory enabling a first level of parallelism between 1) the data exchanges performed by the input/output module and 2) the data encryption and decryption operations performed by the encryption module; and

a second level of parallelism by providing access to data of the dual port memory during parallel operation of both first and second encryption sub-modules.

Claim 15 – presented as amended without markup (for Examiner's convenience):

15. (currently amended) An encryption circuit for simultaneously processing various encryption algorithms, the encryption circuit adapted to be coupled to a host computer system, the encryption circuit comprising:

an input/output module coupled to the host computer system through a dedicated bus,

the input/output module handling data exchanges between the host system and the encryption circuit,

the input/output module comprising a microcontroller and a microcontroller control memory, the microcontroller control memory providing storage for program control of the microcontroller;

an encryption module performing data encryption and decryption operations, as well as storage of all sensitive information of the encryption circuit; and

isolation means comprising a dual port memory connected between the input/output module and the encryption module, the isolation means ensuring that the sensitive information stored in the encryption module is inaccessible to the host computer system,

the dual port memory enabling parallelism between 1) the data exchanges performed by the input/output module and 2) the data encryption and decryption operations performed by the encryption module.